AO-106 (Rev: 06/09)-Application for Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
the Person of Ryan Thomas Llewellyn

Case No. 24-mj-381-CDL

FILED UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2422(b)	**Coercion and Enticement of a Minor**
18 U.S.C. §§ 2251(d)(1)(A) & 2251(e)	**Advertising to Purchase and Receive Child Pornography**
18 U.S.C. §§ 2252(a)(2) & (b)(2)	**Receipt of Child Pornography**
18 U.S.C. §§ 2252(a)(4)(B) & (b)(2)	**Possession of Child Pornography**

The application is based on these facts:

See Affidavit of Dustin L. Carder attached hereto.

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Dustin L. Carder, HSI
Printed name and title

Subscribed and sworn to by phone.

Date: May 23, 2024

Judge's signature

City and state: Tulsa, Oklahoma

Christine D. Little, U.S. Magistrate Judge
Printed name and title

Affidavit in Support of an Application
Under Rule 41 for a Warrant to Search and Seize

I, Dustin L. Carder, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for three separate search warrants for the person and locations specifically described in Attachment A of this Affidavit, including:

a. Search Warrant 1: the entire property located at 6306 South 107th East Avenue, Apartment #1, Tulsa, Oklahoma 74133, Tulsa County, Northern District of Oklahoma ("Subject Residence");

b. Search Warrant 2: the vehicle described as a tan 2012 Kia Sorento with Oklahoma License Plate GTJ-086, VIN: 5XYKT4A68CG228868 ("Subject Vehicle"); and

c. Search Warrant 3: the person of Ryan Thomas Llewellyn, Date of Birth: xx/xx/1984 ("LLEWELLYN"),

the content of electronic storage devices located therein, for evidence, instrumentalities, contraband, and/or fruits of violations of 18 U.S.C. § 2422(b) (Coercion or Enticement of a Minor), 18 U.S.C. §§ 2251(d)(1)(A) and 2251(e) (Advertising to Purchase and Receive Child Pornography), Title 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt of Child Pornography), and Title 18 U.S.C. §§

2252(a)(4)(B) and (b)(2) (Possession of Child Pornography) which items are more specifically described in Attachment B of this affidavit.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

3. I have been employed as a Special Agent ("SA") with Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI") since December 2018 and am currently assigned to the Office of the Resident Agent in Charge in Tulsa, Oklahoma, and am currently assigned to investigate crimes involving child exploitation. While employed by HSI, I have investigated federal criminal violations related to child exploitation and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center's (FLETC) twelve-week Criminal Investigator Training Program (CITP) and the sixteen-week Homeland Security Investigations Special Agent Training (HSISAT) program, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have received focused child exploitation training covering topics such as: interview techniques, live streaming investigations, undercover investigations, capturing digital evidence, transnational child sex offenders, and

mobile messaging platforms utilized by these types of offenders. I am an investigative officer, or law enforcement officer, of the United States of America within the meaning of 18 U.S.C. § 2510(7) and Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure, that is an officer of the United States who is empowered by law to request search warrants and to conduct investigation of, and make arrests for, offenses enumerated in Title 18. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2422, 2251, 2252, and 2252(a).

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

5. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. § 2422(b) (Coercion or Enticement of a Minor), 18 U.S.C. §§ 2251(d)(1)(A) and 2251(e) (Advertising to Purchase and Receive Child Pornography), Title 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt of Child Pornography), and Title 18 U.S.C. §§

2252(a)(4)(B) and (b)(2) (Possession of Child Pornography) will be located at 6306 South 107th East Avenue, Apartment #1, Tulsa, Oklahoma 74133, Tulsa County, Northern District of Oklahoma, within the tan 2012 Kia Sorento with Oklahoma License Plate GTJ-086, VIN: 5XYKT4A68CG228868, and on the person of Ryan Thomas Llewellyn, as further described in their respective Attachment A.

Jurisdiction

6. "[A] warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States." 18 U.S.C. § 3103a.

7. The requested search is related to the following violations of federal law:

a. Title 18, United States Code, Section 2422(b) which states that whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title and imprisoned not less than 10 years or for life.

b. Title 18, United States Code, Sections 2251(d)(1)(A) and 2251(e) which state that any person who, in a circumstance described in paragraph (2), knowingly makes, prints, or publishes, or causes to be made, printed, or published, any notice or advertisement seeking or offering to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct shall be punished as provided under subsection (e).

c. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) which prohibit any person from knowingly receiving, or distributing, any

visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if— (A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (B) such visual depiction is of such conduct.

d. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) which prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

8. Venue is proper because the location, vehicle, and person to be searched are located within the Northern District of Oklahoma.

Definitions

9. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and the attachments incorporated herein:

a. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production

of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct;

b. "Internet Protocol address" or "IP address" refers to a unique number used by a computer or electronic device to access the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means the ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet;

c. "Electronic Mail," commonly referred to as email (or e-mail), is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. Email systems are based on a store-and-forward model; that is, email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need only connect briefly, typically to an email server, for as long a period of time as it takes to send or receive messages. One of the most commons methods of obtaining an email account is through a free web-

based email service provider such as, Outlook, Yahoo, or Gmail. Anyone with access to the Internet can generally obtain a free web-based email account;

d. A "hash value" or "hash ID" is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names;

e. "Cloud storage service" refers to a publicly accessible, online storage provider that can be used to store and share files in large volumes. Users of cloud storage services can share links and associated passwords to their stored files with others in order to grant access to their file collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop computers, laptops, mobile phones or tablets, from anywhere. Many services provide free access up to a certain size limit;

f. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state;

g. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years;

h. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form;

i. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person; and

j. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

Probable Cause

10. On February 6, 2024, I received a phone call from "J.D.," who had recently discovered inappropriate communications on Snapchat[1] between her 15-year-old daughter and multiple other individuals. J.D. told me that her daughter, the minor victim (MV), had received money for sending explicit content of herself to those individuals and received payment via Cash App[2].

11. On February 8, 2024, SA Erin Staniech and I met with J.D., her husband, and MV in their home in Broken Arrow, Oklahoma. J.D. provided MV's phone to agents for forensic examination. J.D. signed a Consent to Search Form for the phone and MV's Snapchat account. The phone is an Apple iPhone 14 Pro Max, serial number 37QT2WVCC4.

12. Agents briefly spoke with MV with her parents present. MV provided the phone number of one of the suspects, known as "Ryl," as (918) 313-2747. MV stated that Ryl deleted his Snapchat accounts as soon as he received explicit content from her and would then create a new one. MV provided the Cash App handles for herself (redacted), and three suspects as "$jbomb68," "$kylecox20," and "RYL." MV provided one of the suspect's Snapchat usernames as "treywey21." The

[1] Snapchat is an American multimedia instant messaging app and service developed by Snap Inc., originally Snapchat Inc. One of the principal features of Snapchat is that pictures and messages are usually only available for a short time before they become inaccessible to their recipients.

[2] Cash App is a peer-to-peer payment app that lets individuals quickly send, receive and invest money. Block, Inc., formerly Square, Inc., launched the app, initially named Square Cash, in 2013 to compete with mobile payment apps like Venmo and PayPal.

investigation thus far has revealed that only "RYL" is located within the Northern District of Oklahoma. The other targets are located in other states.

13. On February 13, 2024, MV was interviewed at the Child Abuse Network in Tulsa, Oklahoma, by forensic interviewer Karla Cordero. The interview was audio and video recorded. The following is a summary of some of the statements made:

a. MV is 15 years old and in the 9th grade.
b. MV lives with her mother and father.
c. MV was there to talk about what happened on Snapchat.
d. MV was selling her pictures and videos to men on Snapchat.
    i. MV stated their names were "Trey," "Jack Davenport" and "Ry."
    ii. MV provided her Snapchat username.
e. All three individuals randomly added her on Snapchat, and as far as she knows, do not know each other.
f. They asked her if she wanted money for pictures; she said yes.
    i. Ry made multiple accounts and would delete his account after receiving content and would then add her back onto a new account.
    ii. They would ask for pictures of her breasts and butt.
    iii. The pictures to Ry had her face in it and breasts exposed.
g. Everything started with Ry in approximately January-February 2023.
    i. Ry would send her $50-$100 via Cash App for 5-10 pictures.
    ii. One of them also used Apple Pay to send her money. MV thought it was possibly Ry because she had his phone number (listed in paragraph 12).
h. MV stated she never talked to any of them on the phone.

i. She would communicate with them on Snapchat if she needed money and would ask if they want pictures.

j. She told all of them that she was 15; she was actually 14 when she told two of them she was 15.

k. Ry told MV that he lives in Tulsa.

l. Ry offered her $500 to meet up with him and perform oral sex on him, which she declined.

m. MV bought marijuana and games with the money she was sent.

n. MV got in trouble at school for vaping, mom went through her phone and found the messages.

14. On February 13, 2024, prior to the forensic interview, I manually reviewed MV's phone and discovered nude images and videos of what appear to be MV. Her vagina was exposed in multiple files. Messages with Ry were not located; however, messages with another user mentioned by MV were located. These files contained multiple sexually explicit images and videos of MV in which her vagina is exposed.

15. On February 16, 2024, HSI Tulsa electronically served AT&T with an administrative Department of Homeland Security ("DHS") summons for subscriber information for phone number (918) 313-2747 from February 1, 2023, through the present. This phone number was provided by MV as belonging to "Ry L," one of the targets who purchased explicit material from her.

16. AT&T responded the same day and provided the requested information. The listed subscriber is Ryan LLEWELLYN with an address of 1139 South Florence

Avenue, Tulsa, Oklahoma 74104. The account was activated on April 3, 2015, and is still active.

17. I then queried "Ryan Llewellyn" in Tulsa on Accurint[3]. Accurint returned a Ryan Thomas LLEWELLYN associated with phone number (918) 313-2747. LLEWELLYN's date of birth is xx/xx/1984, making him 39 years old. His social security number is listed as xx-xxx-1587. The most recent address associated with LLEWELLYN is **6306 South 107th East Avenue, Apartment 1, Tulsa, Oklahoma 74133**, the Subject Residence. The address of 1139 South Florence Ave in Tulsa is listed in Accurint as a previous address. LLEWELLYN's Oklahoma driver's license, which was issued on February 7, 2022, and expires on January 31, 2026, also lists his address as the Subject Residence.

18. Accurint also revealed a vehicle for LLEWELLYN. It was listed as a **2012 Kia Sorento with Oklahoma license plate GTJ-086, VIN: 5XYKT4A68CG228868**, the Subject Vehicle. Upon searching the vehicle's registration through State of Oklahoma records, I confirmed the vehicle is registered to LLEWELLYN at the Subject Residence. The vehicle was last registered on July 7, 2023, and expires July 31, 2024.

19. After reviewing the minor victim's Cash App activity on her device, I was able to determine "Ry L's" Cash App handle was $ry91888. On or about February 23,

[3] Accurint is online investigative software, similar to CLEAR, that provides law enforcement with a direct connection to public records to help verify identities, assets, and connections.

2024, HSI Tulsa electronically served Block, Inc., owner and operator of Cash App, with an administrative DHS summons for subscriber information associated with Cash App handle $ry91888, and the Cash App handle associated with MV. Information requested in the summons included all records including customer name, identifiers, telephone number(s), IP addresses, registration forms, payment and transactional records, email addresses, deposit records, customer correspondence, and any other data that might assist in identifying the account holder or account activity, emails/phone calls or correspondence with the account holder. It was further requested that Block, Inc. provide any and all linked information on other account customers that are conducting transactions with the potential account holder, accounts that are linked and/or sharing digital fingerprints, device IDs or other data that indicate the account holder. The date range requested was February 1, 2023, through the present.

20. On or about February 27, 2024, Block, Inc. responded to the summons and provided the requested information. Pertaining to the $ry91888 account, believed to be associated with LLEWELLYN, the name, date of birth, and social security number fields were blank. According to the provided documents, this means that the account has not met internal thresholds for identity verification. No address was listed either. Display names for the account are "Ry Llll," and "Ry L." These are the names created by a subscriber for peers to recognize and will show up on transaction records.

21. The below "alias history" for the account refers to any additional $cashtags, phone numbers, email addresses, or aliases that may be connected and/or previously used by the account holder:

Date	Alias	Source	Status
2023-06-24 18:29:12 UTC	ry91888	CASHTAG	Removed
2023-06-24 18:29:12 UTC	bluebyyou714@gmail.com	EMAIL	Removed
2023-06-24 16:22:37 UTC	ry91888	CASHTAG	Added
2023-06-24 16:22:37 UTC	ryryllll	CASHTAG	Removed
2023-06-24 16:22:18 UTC	9183132747	SMS	Removed
2023-06-24 16:22:11 UTC	bluebyyou714@gmail.com	EMAIL	Added
2023-05-06 00:05:13 UTC	ryryllll	CASHTAG	Added
2023-05-06 00:04:09 UTC	9183132747	SMS	Added
2023-04-29 14:51:06 UTC	C_se22paype	CUSTOMER_TOKEN	Added

22. As previously described herein, phone number (918) 313-2747, registered to LLEWELLYN, was used by this Cash App account as an alias.

23. There are multiple successful payment transactions from this account listed below:

Date	Status	Total	Subject	Sender	Sndr. Source	Action	Recipient
2023-08-16 21:40:14 UTC	BILL_GETTER_INVALID	USD 1.00		Ry L	N/A	Request	MV
2023-07-24 23:50:51 UTC	BILL_GETTER_INVALID	USD 1.00	wya	Ry L	N/A	Request	MV
2023-07-11 18:55:51 UTC	BILL_GETTER_INVALID	USD 1.00	when you coming back?	Ry L	N/A	Request	MV
2023-06-24 17:40:06 UTC	PAID_OUT	USD 10.00		Ry L	4223230010746226	Paying	MV
2023-06-24 17:31:03 UTC	PAID_OUT	USD 50.00		Ry L	4223230010746226	Paying	MV
2023-06-24 17:30:47 UTC	DECLINED	USD 50.00		Ry L	6011003532563341	Paying	MV
2023-06-24 17:17:31 UTC	PAID_OUT	USD 1.00	added you-ry_ry9188	Ry L	4223230010746226	Paying	MV

2023-06-24 17:13:05 UTC	PAID_OUT	USD 1.00	don't see anything	MV	CASH_BALANCE	Paying	Ry L
2023-06-24 17:11:29 UTC	PAID_OUT	USD 5.00	check snap	Ry L	6011003532563341	Paying	MV
2023-06-24 17:10:43 UTC	PAID_OUT	USD 5.00	😊	Ry L	6011003532563341	Paying	Angi eee Luvv
2023-06-24 16:25:51 UTC	PAID_OUT	USD 25.00	🤣	Ry L	6011003532563341	Paying	Angi eee Luvv
2023-05-17 02:09:07 UTC	PAID_OUT	USD 50.00	😁	Ry L	4223230010746226	Paying	Staci a Rosso

24. As seen above, on June 24, 2023, "Ry L" paid MV $10. It appears he also attempted to send MV $50, which was declined; he then sent MV $1 with a note that he had added her [on Snapchat], and his username was ry_ry9188. This Snapchat account no longer exists. The $1 was returned to Ry L by MV with a note that said she did not see anything. Ry L then sent MV another successful transaction of $5 with a note to "check snap." Ry L has payments totaling $80 to other unknown females during this timeframe as well.

25. Pertaining to MV's Cash App account, there is identifying information returned in the data associated with MV's mother and MV, positively linking the account to MV. The email address and phone number linked to MV and this Cash App account will not be listed to protect MV's identity, as the email address contains her actual name. Payment transactions associated with Ry L were located in MV's Cash App data as well, as outlined below:

Date	Status	Total	Subject	Sender	Sndr. Source	Action	Recipient
2023-08-16 21:40:14 UTC	BILL_GETTER_INVALID	USD 1.00		Ry L	N/A	Request	MV
2023-07-24 23:50:51 UTC	BILL_GETTER_INVALID	USD 1.00	wya	Ry L	N/A	Request	MV
2023-07-11 18:55:51 UTC	BILL_GETTER_INVALID	USD 1.00	when you coming back?	Ry L	N/A	Request	MV
2023-06-24 17:40:06 UTC	PAID_OUT	USD 10.00		Ry L	4223230010746226	Paying	MV
2023-06-24 17:31:03 UTC	PAID_OUT	USD 50.00		Ry L	4223230010746226	Paying	MV

2023-06-24 17:30:47 UTC	DECLINED	USD 50.00		Ry L	6011003532563341	Paying	MV
2023-06-24 17:17:31 UTC	PAID_OUT	USD 1.00	added you-ry_ry9188	Ry L	4223230010746226	Paying	MV
2023-06-24 17:13:05 UTC	PAID_OUT	USD 1.00	don't see anything	MV	CASH_BALANCE	Paying	Ry L
2023-06-24 17:11:29 UTC	PAID_OUT	USD 5.00	check snap	Ry L	6011003532563341	Paying	MV
2023-02-02 05:08:36 UTC	PAID_OUT	USD 50.00		Ryan	4223230010746226	Paying	MV

26. MV's transaction history with Ry L mirror what was located in Ry L's. The only thing different was that an additional transaction of $50 from "Ryan" to MV was paid out on February 2, 2023. The debit or credit card number linked to "Ryan's" account is the same number that linked to other successful payments to MV from Ry L, indicating that "Ry L," and "Ryan" are the same individual.

27. On March 14, 2024, HSI Tulsa electronically served Google with an administrative DHS summons for subscriber information associated with email address "bluebyyou714@gmail.com," which was used as an alias for the $ry91888

Cash App account, for a date range of February 1, 2023, through the present. Google responded to the summons the same day and provided the requested information.

28. The name associated with the email account, as entered by the user, is Thomas Quinn. There were no phone numbers or other email addresses associated with the account. There were, however, IP addresses utilized by the account, with the most recent being 2600:8804:5c02:7800:1925:2ee4:da8:e7e0 on 2024-03-12 03:14:19 Zulu Time (similar to UTC). This IP address shows to be serviced by Cox Communications.

29. In the provided Google billing information, I observed that the same debit or credit card used by "Ry L" to send money to MV is also linked to this Google account. The account holder and billing name listed here is Ryan LLEWELLYN. On the 'Customer Info' text file, LLEWELLYN's name is listed again as a recipient in the 'Postal Address' section; however, his address is not listed. It does list a zip code of 74133, which is the zip code of the Subject Residence.

30. According to open source www.maxmind.com, IP address 2600:8804:5c02:7800:1925:2ee4:da8:e7e0 geolocates to Tulsa, Oklahoma, and is serviced by Cox Communications. On or about April 8, 2024, HSI Tulsa electronically served Cox Communications with an administrative DHS summons for subscriber information associated with the IP address on March 12, 2024, at 03:14:19 Zulu Time (UTC).

31. On or about April 23, 2024, Cox Communications responded to the summons and provided the requested information:

Subscriber Information:
Name: RYAN LLEWELLYN
Address: APT 1 6306 S 107TH EAST AVE TULSA, OK 74133
Telephone: 918 313-2747
Email address/es: ryryllll@yahoo.com
Account / Service Information
Account Number: 186012412914
Type of Service: HIGH SPEED DATA SERVICES (ACTIVE)
Account Start Date: 12/31/2019
Disconnect Date: N/A

32. As noted above, the registered subscriber of the IP address is Ryan LLEWELLYN at the Subject Residence. The listed phone number for LLEWELLYN as provided by Cox Communications matches the phone number for "Ry L" as provided by MV. As described herein, the registered AT&T subscriber of this phone number is LLEWELLYN. The internet account still shows to be active. The email address "ryryllll@yahoo.com" was previously unknown to me; however, "ryryllll" was also listed as an alias used on the target's Cash App account.

33. A check of LLEWELLYN's employment records through the Oklahoma Employment Security Commission revealed that he worked for GFP Acquisition Company; Address: 440 S La Salle St Ste 3100, Chicago, IL 60605; Location: 2701 W Concord Street, Broken Arrow, OK 74012; Phone Number: (918) 317-0401. This company is listed as an HVAC company. Upon querying the Broken Arrow address,

I learned that the address is associated with American Wheatley, an HVAC parts manufacturer.

34. On May 14, 2024, at approximately 0800 hours, I observed the Subject Vehicle parked at American Wheatley in Broken Arrow, OK. On May 15, 2024, at approximately 1700 hours, while conducting surveillance near American Wheatley, I observed LLEWELLYN driving the Subject Vehicle after leaving work. LLEWELLYN stopped at the QuikTrip located at 2400 N Aspen Ave, Broken Arrow, OK, and went inside. I took photographs of LLEWELLYN as he exited the store and entered his vehicle again. I was able to positively identify LLEWELLYN as the driver based on previously viewing his Oklahoma driver's license photograph.

35. I then traveled to the Subject Residence ahead of LLEWELLYN. Approximately twenty minutes later, I observed and took photographs of LLEWELLYN arriving back at the Subject Residence. LLEWELLYN parked directly in front of the walkway to Apartment 1, in front of building 6306. LLEWELLYN exited the Subject Vehicle and walked towards Apartment 1, where he disappeared from view. Apartment 1 is the only apartment located in the area LLEWELLYN walked to. I then terminated surveillance.

36. Due to the successful Cash App transactions between LLEWELLYN and MV, MV's statements in her forensic interview, and the sexually explicit images and videos observed on MV's device sent to others, I believe that the evidence described

in Attachment B will be located in the places described in their respective Attachment A.

Characteristics Common to Individuals Who Exhibit a Sexual Interest in Children

37. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who exhibit a sexual interest in children:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity;

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;

c. Such individuals typically possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in a secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years;

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis;

e. Based on my training and experience and speaking with other special agents, I know that such individuals have taken their electronic devices and storage media, which contain their collections of child pornography, with them when they have moved or changed residences;

f. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings. These images, videos or other recordings may be taken or recorded covertly, such as with a

hidden camera in a bathroom, or the individual may have child victims he or she is abusing in order to produce child pornographic or child erotica images, videos or other recordings. These images, videos or other recordings are often collected, traded, or shared;

g. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted"[4] it;

h. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography;

i. Such individuals may use social media applications or other means of electronic communications to locate, converse with, and groom minor victims in an attempt

[4] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

to solicit child pornography and/or physically meet and sexually abuse a minor victim;

j. Such individuals who use social media applications or other means of electronic communications to locate, converse with, and groom minor victims often do not just have one victim. It has been my experience in these types of investigations that such individuals will communicate with multiple victims in an attempt to be more successful in obtaining child pornography and/or physically meeting and abusing a victim;

k. Such individuals prefer not to be without their child pornography for any prolonged period of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if LLEWELLYN uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the Subject Residence, and/or the Subject Vehicle, and/or the person of LLEWELLYN as set forth in their respective Attachment A.

Background on Child Pornography, Computers, and the Internet

38. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers, smartphones[5] and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers and smartphones basically serve four functions in connection with child pornography: production, communication, distribution, and storage;

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos;

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other

[5] Smartphones are a class of mobile phones and of multi-purpose mobile computing devices. They are distinguished from feature phones by their stronger hardware capabilities and extensive mobile operating systems, which facilitate wider software, internet (including web browsing over mobile broadband), and multimedia functionality (including music, video, cameras, and gaming), alongside core phone functions such as voice calls and text messaging.

computers via wireless connections. Electronic contact can be made to literally millions of computers and smartphones and tablets around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone;

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also almost always carried on an individual's person (or within their immediate dominion and control) and can additionally store media;

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion;

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing

service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases; and

g. As is the case with most digital technology, communications by way of computer or smartphone can be saved or stored on the computer or smartphone used for these purposes. Storing this information can be intentional (i.e., by saving an e-mail as a file on the computer or smartphone, or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer or smartphone user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Specifics of Search and Seizure of Computer Systems

39. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Subject Residence, and/or the Subject

Vehicle, and/or the person of LLEWELLYN in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, such as a cellular phone, smartphone, or tablet. Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

40. I submit that if a computer or storage medium is found on the Subject Residence, and/or the Subject Vehicle, and/or the person of LLEWELLYN, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data;

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file;

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information;

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

41. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrants, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Residence, and/or the Subject Vehicle, and/or the person of LLEWELLYN because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of

a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified;

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the

search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that logs the following: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant

insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement);

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when;

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant;

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence

of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent;

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

42. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of computer systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, smartphones, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of

the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

43. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an

alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

44. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrants.

Conclusion

45. Based on the information set forth in this affidavit, I submit there is probable cause to believe that 18 U.S.C. § 2422(b) (Coercion or Enticement of a Minor), 18 U.S.C. §§ 2251(d)(1)(A) and 2251(e) (Advertising to Purchase and Receive Child Pornography), Title 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt of Child Pornography), and Title 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of Child Pornography) have been violated, and that the contraband, property, evidence, fruits and instrumentalities of this offense, more fully described in Attachment B, are located at the sites described in their respective Attachment A. I respectfully request that this Court issue search warrants for the locations described in their respective Attachment A, authorizing the search and seizure of the items described in Attachment B.

46. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab; digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Respectfully submitted,

Dustin L. Carder
Special Agent
Homeland Security Investigations

Subscribed and sworn to by phone this 23rd day of May, 2024.

CHRISTINE D. LITTLE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

This warrant applies to the person of Ryan Thomas Llewellyn, date of birth xx/xx/1984, and social security number xxx-xx-1587, who is listed on his/her driver's license as 5'6" tall, weighing 210 pounds, is bald, with brown eyes, and who is pictured below:

ATTACHMENT B

Particular Things to be Seized

All items that constitute evidence, instrumentalities, contraband, and/or fruits of violations of 18 U.S.C. § 2422(b) (Coercion or Enticement of a Minor), 18 U.S.C. §§ 2251(d)(1)(A) and 2251(e) (Advertising to Purchase and Receive Child Pornography), Title 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt of Child Pornography), and Title 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of Child Pornography) involving LLEWELLYN, including:

A. Images/videos/gifs of child pornography or child erotica; files containing images/videos/gifs; and data of any type relating to the sexual exploitation of minors or a sexual interest in children, material related to the possession thereof, and data of any type related to any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting such visual depiction of such conduct, in any form wherever it may be stored or found including, but not limited to:

i. Any cellular telephone, smartphone, tablet, personal digital assistant, computer, computer system and related peripherals; computer hardware; computer software; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer

printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, monitors, printers, external storage devices, routers, modems, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to computer passwords and data security devices and computer-related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography];

ii. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

iii. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children; and

iv. Stories, text-based files, motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

B. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors or a sexual interest in children, that were transmitted or received using computer, cellular device, personal digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, Cash App transactions and other digital financial records, and electronic messages, establishing possession, access to, or

transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

ii. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

iii. Any and all records, documents, or materials, including any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

iv. Any and all records, documents, or materials, including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors or a sexual interest in children;

v. Any and all records of Internet usage including user names and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums, including CDs or DVDs];

vi. Any physical keys, encryption devices, dongles and similar physical items necessary to access computer equipment, storage devices or data;

vii. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and

viii. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software];

C. Credit card information including, but not limited to, bills and payment records, and including, but not limited to, records of internet access;

D. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence;

E. Records or other items which evidence ownership or use of computer equipment or any of the devices described in this attachment that are found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes;

F. Any and all adapters, chargers, or other hardware items necessary to charge the battery, or to maintain the functioning of, any of the equipment described above; and

G. Any data or materials establishing ownership, use or control of any computer equipment seized from 6306 South 107th East Avenue, Apartment #1, Tulsa, Oklahoma 74133, and the Subject Vehicle.

H. Any and all information, correspondence (including emails and text messages), records, documents and/or other materials related to contacts, in whatever form, with minors involving the production, possession and/or distribution of child pornography and the attempt or act of educing, enticing, coercing, or persuading a minor to engage in sexual acts, and the advertisement and/or purchase of child pornography.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.